



National Airspace System Communication System Safety Hazard Analysis and Security Threat Analysis

**Version 1.0
21 February 2006**

TABLE OF CONTENTS

| | |
|---|-----------|
| EXECUTIVE SUMMARY | 3 |
| 1 OVERVIEW | 4 |
| 1.1 INTRODUCTION..... | 4 |
| 1.1 GOAL AND OBJECTIVES..... | 4 |
| 1.2 PROCESS..... | 4 |
| 1.3 ANALYSIS SCOPE | 5 |
| 1.4 ASSUMPTIONS AND CAVEATS..... | 5 |
| 1.5 DOCUMENTING THE CURRENT NAS COMMUNICATION SYSTEM..... | 6 |
| 1.5.1 Functional Analysis | 6 |
| 1.5.2 Physical Architecture..... | 6 |
| 1.6 INTEGRATING SAFETY AND SECURITY | 7 |
| 2 SAFETY HAZARD ANALYSIS | 10 |
| 2.1 SAFETY ANALYSIS PROCESS | 10 |
| 2.2 SAFETY ANALYSIS | 10 |
| 2.2.1 Describing the NAS Communication System..... | 10 |
| 2.2.2 Identifying the NAS Communication System Safety Hazards | 10 |
| 2.2.3 Analyzing the NAS Communication System Safety Risk | 13 |
| 2.2.4 Assessing NAS Communication System Safety Risks | 21 |
| 2.2.5 Treating NAS Communication System Safety Risks..... | 21 |
| 2.3 SAFETY ANALYSIS CONCLUSIONS | 21 |
| 3 SECURITY THREAT ANALYSIS..... | 23 |
| 3.1 NAS COMMUNICATION SYSTEM SECURITY ANALYSIS PROCESS | 23 |
| 3.2 SECURITY ANALYSIS | 28 |
| 3.2.1 Threat Identification | 28 |
| 3.2.2 Existing NAS Communication System Security Controls..... | 31 |
| 3.2.3 Assessing NAS Communication System Security Risk..... | 32 |
| 3.2.4 Treating NAS Communication System Security Risk..... | 32 |
| 3.3 Security Analysis Conclusions | 33 |

TABLE OF TABLES

| | | |
|------------|---|----|
| Table 1-1: | Comparable Deliverables for Safety and Security Processes | 8 |
| Table 2-1: | Functional Hazard Categorization | 12 |
| Table 2-2: | Safety Severity Categories..... | 13 |
| Table 2-3: | Existing NAS Communication System Safety Controls..... | 14 |
| Table 2-4: | Safety Likelihood Categories..... | 19 |
| Table 2-5: | NAS Communication System Safety Risk Summary | 20 |
| Table 3-1: | Security Severity Categories..... | 25 |
| Table 3-2: | Security Likelihood Categories..... | 27 |
| Table 3-3: | Security Risk Assessment Matrix | 28 |
| Table 3-4: | Security Threats to Existing NAS Communication System | 29 |
| Table 3-5: | Existing Security Controls | 31 |

TABLE OF FIGURES

| | | |
|-------------|--|----|
| Figure 1-1: | Generic Physical Architecture for the NAS Communication System | 7 |
| Figure 1-2: | Safety and Security Process Commonalities..... | 8 |
| Figure 2-1: | SMS Safety Analysis Process used in NAS Communication System Safety Analysis | 10 |
| Figure 2-2: | Predictive Risk Matrix | 19 |
| Figure 3-1: | The Security Threat Analysis Process | 24 |

Executive Summary

The Federal Aviation Administration (FAA) Air Traffic Organization (ATO) has established procedures to provide a baseline for both the safety and security of the operational National Airspace System (NAS) Communication System. Each program chartered to implement or modify operational systems will have to perform detailed safety and security analyses and thoroughly document the supporting evidence for these analyses. To evaluate the completeness and validity of these analyses, from a high level perspective and in a consistent manner, a documented safety and security baseline for the current NAS Communication System was deemed necessary. This document presents a high level analysis of the safety and security aspects of the current NAS Communication System, to accomplish the following objectives:

1. Identify hazards and threats,
2. Identify risk from both safety and security viewpoints,
3. Identify assumptions used in the analyses,
4. Provide a functional and architectural view of the current NAS Communication System upon which to base future safety and security analyses, and
5. Provide documentation to facilitate future safety and security analyses.

Safety examines risk resulting from unintentional causes, while security primarily involves risk resulting from intentional causes. Safety and security practitioners within the FAA use different processes to determine safety and security risks. The safety hazard analysis in this document used the Safety Management System five step process. The security threat analysis was adapted from the FAA's SCAP [12] and from the National Institute of Standards and Technology's (NIST) standards and guidelines for the implementation of the Federal Information Security Management Act (FISMA) requirements. Regular team coordination of interim safety and security products minimized discrepancies and issues throughout the analysis.

Specific coordination points are identified in the following table:

| Safety Hazard Analysis | Security Threat Analysis |
|--|---|
| Describe System - Functional Analysis | Describe System - Functional Analysis - Physical Architecture - Security Categorizations |
| Identify Hazards | Identify Threats |
| Analyze Risks - Identify Existing Controls | Analyze Security Risks - Identify Existing Controls |
| Assess Risk (Severity and Likelihood) | Assess Threat (Severity and Likelihood) |
| Treat Risk (this may include identifying new safety requirements) | Treat Risk (this may include identifying new security requirements) |

This baseline did not identify any high level unacceptable risks for safety or security for FAA management to consider. However, the security analysis did identify a need for a detailed security analysis.

1 Overview

1.1 Introduction

The FAA reorganized in 2003 and created a new Air Traffic Organization (ATO) by combining the services performed by Air Traffic Services (ATS), Research and Acquisitions (ARA), and Free Flight (AOZ). Safety is the ATO's first priority. Formal implementation of a Safety Management System (SMS), consistent with international models, is currently in progress. The ATO Safety Service Unit works directly with the FAA Air Traffic Safety Oversight Service to define safety critical systems and the process to ensure that any hardware or software changes to the National Airspace System (NAS) are preceded by the identification, implementation, and evidence of the appropriate safety measures. The FAA declared the current NAS is acceptable from a safety standpoint. Additionally, in the post September 11 era, the FAA elevated concerns over the correct level of security required to adequately protect the hardware and software systems present in the NAS. The FAA has subsequently implemented security controls to address some of the concerns.

In response, the Technical Operations, Air Traffic Control (ATC) Communications Services established a Safety and Security Task Force (SSTF) to identify the safety and security baselines for the current (February 2006) NAS Communication System. The SSTF consisted of members from Technical Operations Services (ATO-W), En-Route and Oceanic Services (ATO-E), the Regulation and Certification Service (AVS), and supporting staff. The SSTF members (see Appendix I) included specialists in air traffic operations, systems engineering, communications engineering, safety engineering, security engineering, technical requirements, flight standards, and certification.

1.1 Goal and Objectives

The goal of the SSTF was to identify the safety and security baselines for the current NAS Communication System to accomplish the following objectives:

1. Identify risks in the current NAS Communication System from both safety and security viewpoints,
2. Identify the assumptions made and provide the analyses for organizational use to expedite the safety and security analyses required for proposed changes, and
3. Provide a consistent functional and architectural view of the current NAS Communication System upon which to base future safety and security analyses.

1.2 Process

There are several activities which were necessary precursors to identifying the safety and security baselines:

1. Defining the boundaries of the current NAS Communication System to be included in the study. This is discussed in Section 1.3.
2. Enumerating the assumptions which will be used in the study as discussed in Section 1.4.
3. Documenting the current NAS Communication System
 - Functional Analysis as discussed in Section 1.5.1.
 - Physical Architecture as discussed in Section 1.5.2.

Once these activities were completed the main portion of study was initiated.

There were lengthy discussions in an attempt to combine the safety and security analysis. The net result was to pursue each analysis, with separate teams, but to frequently interchange results. A further discussion of integrating safety and security is in Section 1.6.

The safety analysis is detailed in Section 2. The security analysis is detailed in Section 3. The acronyms and definitions used in the report are contained in Appendix G. A list of references is provided in Appendix H.

1.3 Analysis Scope

In order to conduct safety and security analyses of the NAS Communication System, the SSTF first had to “bound” the system. Bounding the system helps the team focus on hazards and issues that directly impact the analysis. Items which are “in-bounds” must be considered in the analysis process.

In-bounds of the analysis:

- only the communications used for the provision of ATS,
- both voice and data as used in the current system.

Out-of-bounds of the analysis:

- the hazards attributable to a controller or pilot or automation (e.g., the HOST system),
- navigation systems including the associated supporting communications (e.g., Telco)
- surveillance systems including the associated supporting communications (e.g., Telco)
- future services (e.g., domestic Controller Pilot Data Link Communication (CPDLC))
- Occupational Safety Hazards Administration (OSHA) hazards.

1.4 Assumptions and Caveats

The SSTF used the following assumptions and caveats to conduct the safety hazard analysis:

- The safety baseline developed as a result of this study is at a high-level and therefore does not replace detailed safety analyses.
- Safety hazards include only those that are “unintentional”, and intentional hazards are assumed to be part of security.
- Hazard causes are restricted to the NAS Communication system (e.g., failures due to the controller, pilot, surveillance, out-of-conformance detection, and potential conflict indication are not considered.)
- Only single failures were considered (e.g., an air-ground communication failure, assumes that ground-ground communication remains intact; a hazard due to the corruption of an up-linked air-ground message assumes that the down-linked response message is not corrupted).

The SSTF used the following assumptions and caveats to conduct the security analysis:

- The security baseline developed as a result of this study is at a high-level and therefore does not replace detailed security analyses.
- The security baseline assumes that security controls are used in accordance with established policies. (*Note: Audit of how security controls are used in the field would be a valuable future effort.*)
- “Communications control sites” (e.g., Air Route Traffic Control Centers (ARTCCs), Terminal Radar Approach Control (TRACONs)) were assumed to provide sufficient physical access control to prevent outsider attacks on the equipment inside, while “communications edge sites” (e.g., Remote Communication Air/Ground (RCAG), Backup Emergency Communication (BUEC)) were considered to provide only limited physical protection.
- Classified systems (e.g., linking the FAA and Department of Defense (DoD)) have their own security assessment process and for the purposes of this work have been assumed to provide effective security.

1.5 Documenting the Current NAS Communication System

To provide a common framework and to identify key areas for the safety and security analyses, the SSTF conducted a two part high-level description of the current NAS Communication System: a functional analysis and description of the physical architecture.

1.5.1 Functional Analysis

The NAS Communication System safety hazard analysis was based on the functional analysis. At a high level, the following NAS Communication System functions were identified.

- Use the NAS Communication System to send/receive messages:
 - Send/receive fixed to mobile (aircraft/vehicle) messages
 - Send/receive mobile to fixed messages
 - Send/receive fixed to fixed messages,
 - Send/receive mobile to mobile messages, and
- Provide the NAS Communication System, including:
 - Monitor the NAS Communication System,
 - Maintain the NAS Communication System, and
 - Configure the NAS Communication System.

An expanded NAS Communication System functional breakdown is provided in Appendix B. NAS Communication System functions were documented, although not all functions necessarily have safety or security impacts.

1.5.2 Physical Architecture

To perform the security analysis a high-level NAS Communication System physical architecture was also required. For example, the security analysis considered distinct vulnerabilities for systems at manned vs. unmanned locations. A high level depiction of the NAS Communication

System is shown in Figure 1-1. A documented description of the physical architecture is in Appendix C.

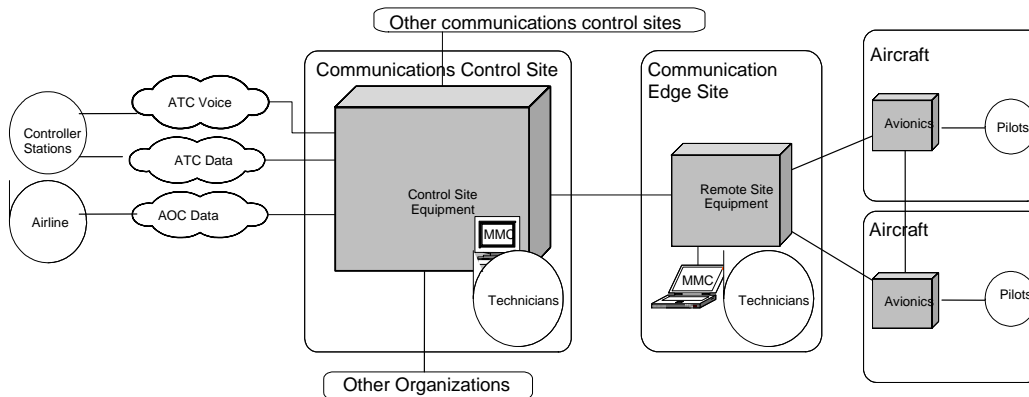


Figure 1-1: Generic Physical Architecture for the NAS Communication System

1.6 Integrating Safety and Security

The disciplines of safety and security have much in common. Both are concerned with identification and assessment of events, which could have an adverse impact on the operation of a system.

The main distinction between safety and security is in the nature of the events that each considers. Safety is traditionally concerned with unintentional events, while security is traditionally primarily concerned with deliberate events. From a safety perspective, the threats that concern security are another potential cause of safety hazards, while from a security perspective; the hazards that concern safety are another potential outcome of security threats.

Given the similarities between safety and security, it is not surprising that the analysis processes traditionally used by the disciplines are also similar. Figure 1-2 below shows the processes at a high-level in order to emphasize these similarities.

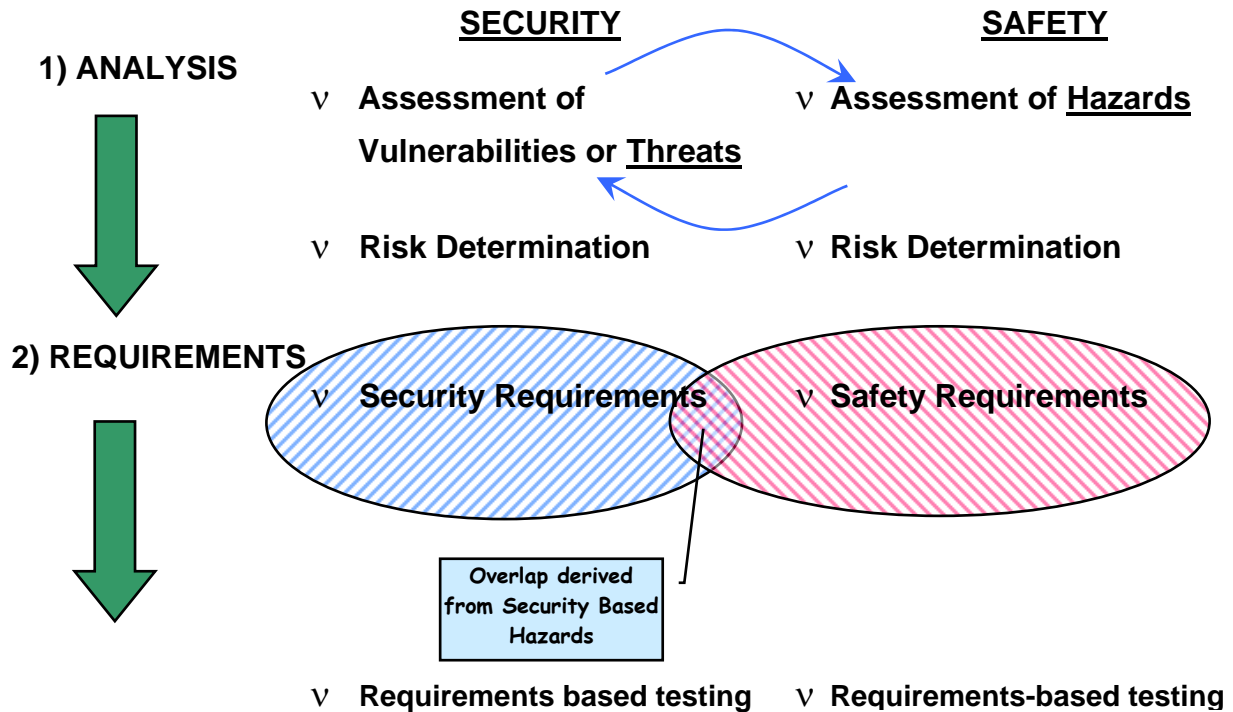


Figure 1-2: Safety and Security Process Commonalities

Table 1-1 below develops the theme of commonality, with each row showing comparable deliverables at various points in the safety and security processes.

Table 1-1: Comparable Deliverables for Safety and Security Processes

| Safety Hazard Analysis | Security Threat Analysis |
|--|---|
| Describe System - Functional Analysis | Describe System - Functional Analysis - Physical Architecture - Security Categorizations |
| Identify Hazards | Identify Threats |
| Analyze Risks - Identify Existing Controls | Analyze Security Risks - Identify Existing Controls |
| Assess Risk (Severity and Likelihood) | Assess Threat (Severity and Likelihood) |
| Treat Risk (this may include identifying new safety requirements) | Treat Risk (this may include identifying new security requirements) |

Based on the similarities between the safety and security processes outlined above, as well as the direction given to the analysis effort to align safety and security as much as possible, the first option considered during analysis planning was complete integration of the safety and security process into a single combined process. This approach was not used for a number of reasons:

- FAA safety and security processes are driven by laws, regulations, policies and guidelines mandated by completely different cognizant organizations both within and outside of the

agency. A combined process will simply not be able to comply with these different drivers unless the drivers themselves are first adjusted.

- Security traditionally considers impact of many different types – including economic impact, business impact, and the like – in addition to safety impact. These other aspects of security would likely be lost in a combined process.
- The adversarial nature of security makes precise estimation of threat severity and likelihood problematic if not impossible – as a result security typically uses qualitative estimates rather than the quantitative estimates favored in the safety world. This distinction makes development of unified severity and likelihood definitions problematic.
- The time and resources assigned to the analysis effort simply did not permit the extensive integration work involved in producing a single combined process.

Instead the approach taken was to pursue separate, but coordinated safety and security analyses. The safety hazard analysis used the SMS Manual five step process. The security threat analysis process used was adapted FAA's Security Certification and Authorization Package (SCAP) and from the National Institute of Standards and Technology's standards and guidelines for the implementation of the Federal Information Security Management Act (FISMA) requirements. Adjustments were made to the security threat analysis process to align it as much as possible with the safety process, and to account for the high-level, rather than component-level nature of the study. In particular the following coordination activities were performed:

- A common functional breakdown of the NAS communications system was developed and used as a starting point by both safety and security. This breakdown is described in Appendix A.
- The safety hazards that could be caused by each security threat were identified, and threat severity was then assigned based primarily on the hazard classes of the associated hazards. The mapping between threats and hazards is described in Appendix F. (The safety hazards in Appendix D do not include security-based causes.)
- New requirements identified by safety and security were coordinated in order to ensure that a minimal set of new requirements was developed, and to ensure that new security requirements did not adversely impact safety and vice versa.

In addition regular meetings were held involving the safety team and the security team in order to identify and exploit any other opportunities for coordination as they arose.

2 Safety Hazard Analysis

This section discusses the safety hazard analysis that was performed on the existing NAS Communication System.

2.1 Safety Analysis Process

The safety analysis process applied is consistent with the System Safety Management Program (SSMP), version 10 [1] and SMS/Safety Risk Management (SRM) [2]. While the methodology applied herein is not a formal SRM process and will not result in a Safety Risk Management Document, the intent is to establish a safety baseline that is SMS/SRM-compatible so that future safety analyses may be done more easily and efficiently with SMS/SRM.

Figure 2-1 shows the 5 step SRS/SRM process used to perform the safety analysis. In this section of the document each of the 5 steps is applied to the NAS communication System and a summary of the result is presented. Details of the safety analysis are contained in Appendices to this document and referenced as appropriated in each step of the safety process.

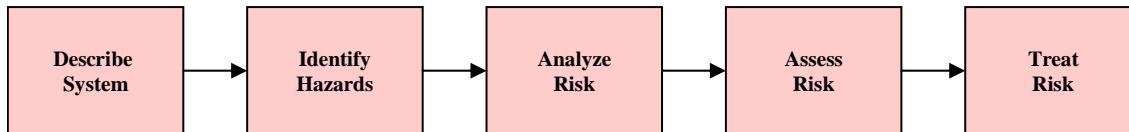


Figure 2-1: SMS Safety Analysis Process used in NAS Communication System Safety Analysis

2.2 Safety Analysis

2.2.1 Describing the NAS Communication System

The first step in the safety analysis is to describe the system. For the NAS Communication System this consisted of conducting a functional analysis (depicted as block diagrams in Appendix A and shown hierarchically in Appendix B). The functional analysis was then used as the basis for the safety hazard analysis.

***Note:** The functional analysis was used by both safety and security in order to maximize commonality between the two disciplines.*

2.2.2 Identifying the NAS Communication System Safety Hazards

The second step is to identify the safety hazards and determine the causes of each hazard. For the NAS Communication System, fifteen safety hazards categories were identified and examined as follows:

- hazards due to lack of availability of the NAS Communication System,
 1. NAS Communication Capability Totally Unavailable – NAS ATS failure,
 2. NAS Communication Capability Partially Unavailable – NAS ATS failure,
 3. NAS Communication Capability Unavailable – Sender to Recipient of NAS ATS Unavailable
- hazards due to failures of the NAS Communication System,

4. NAS communication fails (e.g., aborts) with a given recipient for a single message
5. NAS communication fails (e.g., aborts) with multiple recipients for a single message per aircraft
- hazards due to mis-delivery of a message by the NAS Communication System,
 6. The recipient accepts a message affecting separation from a NAS ATS that is not its control authority.
 7. The recipient accepts a message NOT affecting separation from a NAS ATS that is its control authority.
 8. A message affecting separation gets to unintended recipient.
 9. A message NOT affecting separation gets to unintended recipient
- hazards due to late delivery of a message by the NAS Communication System,
 10. Message affecting separation received too late (or expired)
 11. Message NOT affecting separation received too late (or expired)
- hazards due to corruption of message by the NAS Communication System, and
 12. A message affecting separation corrupted
 13. A message NOT affecting separation corrupted
- hazards due to messages arriving out-of-sequence due to the NAS Communication System.
 14. A message affecting separation sent/received out of sequence
 15. A message NOT affecting separation sent/received out of sequence

These fifteen hazard categories were then applied to each of the high level NAS Communication System functions as follows:

Transceive Fixed to Mobile Message

1. ATS to Airborne Aircraft Message
2. ATS to On-Ground Aircraft Message
3. ATS to Vehicles Message

Transceive Mobile to Fixed Message

4. Airborne Aircraft to ATS Message
5. On-Ground Aircraft to ATS to Message
6. Vehicles to ATS Message

Transceive Fixed to Fixed Message

7. Internal NAS ATS Intrafacility Message
8. Internal NAS ATS Interfacility Message
9. NAS ATS to Other Government Agency (OGA) Message
10. OGA to NAS ATS Message
11. NAS ATS to Foreign ATS Message
12. Foreign ATS to NAS ATS Message

13. NAS ATS to non-NAS/non-OGA Message
14. Non-NAS/non-OGA to NAS ATS Message

Transceive Mobile to Mobile Message

15. Airborne Aircraft to Airborne Aircraft Message
16. Airborne Aircraft to On-Ground Aircraft Message
17. On-Ground Aircraft to Airborne Aircraft Message
18. Airborne Aircraft to Vehicles Message
19. Vehicles to Airborne Aircraft Message
20. On-Ground Aircraft to On-Ground Aircraft Message
21. On-Ground Aircraft to Vehicle Message
22. Vehicle to On-Ground Aircraft Message
23. Vehicle to Vehicle Message

When examining each of the 23 functions, it was found that it was more effective to combine some of the functions, since the safety hazard analysis was the same for the combined functions. The functions were combined as shown in Table 2-1.

Table 2-1: Functional Hazard Categorization

| Functional Area | Hazard Category | Combined Functions |
|--|---|---|
| Fixed to Mobile Message Mobile to Fixed Message | 1 NAS ATS – Aircraft Message Hazards | ATS to Airborne Aircraft Message Airborne Aircraft to ATS Message ATS to On-Ground Aircraft Message On-Ground Aircraft to ATS to Message |
| | 2 NAS ATS –Vehicle Message Hazards | ATS to Vehicle Message Vehicles to ATS Message |
| Fixed to Fixed Message | 3 NAS Intrafacility Message Hazards | Internal NAS ATS Intrafacility Message |
| | 4 NAS Interfacility Message Hazards | Internal NAS ATS Interfacility Message |
| | 5 NAS ATS - OGA Message Hazards | NAS ATS to Other Government Agency (OGA) Message (9) OGA to NAS ATS Message (10) |
| | 6 NAS ATS – Foreign ATS Message Hazards | NAS ATS to Foreign ATS Message Foreign ATS to NAS ATS Message |
| | 7 NAS ATS – Non NAS/Non OGA Message Hazards (e.g., AOC) | NAS ATS to non-NAS/non-OGA Message Non-NAS/non-OGA to NAS ATS Message |

| | | |
|---------------------------------|--|--|
| Mobile to Mobile Message | 8 Aircraft – Aircraft Message Hazards | Airborne Aircraft to Airborne Aircraft Message Airborne Aircraft to On-Ground Aircraft Message On-Ground Aircraft to Airborne Aircraft Message On-Ground Aircraft to On-Ground Aircraft Message |
| | 9 Aircraft – Vehicle and Vehicle – Vehicle Message * *No ATS message were identified; and consequently no hazards apply | Airborne Aircraft to Vehicles Message Vehicles to Airborne Aircraft Message On-Ground Aircraft to Vehicle Message Vehicle to On-Ground Aircraft Message Vehicle to Vehicle Message |

Thus, based on the functional categorization, 120 NAS Communication System safety hazards were identified. (15 hazard categories applied to each of 8 functional categories.) Details of the identified hazards and the safety causes of each hazard are presented in Appendix D. (Security causes of hazards are presented in Appendix F.)

2.2.3 Analyzing the NAS Communication System Safety Risk

The third step is to analyze the system risk. For each of the identified NAS Communication System Safety Hazards (summarized in Section 2.2.2 and detailed in Appendix D) the severity of consequence (i.e., what is the worst thing that can credibly happen) was determined. This was done by determining a system state for each hazard that could lead to the worst credible effect occurring and then tracing a scenario(s) that could result should the hazard occur. The criteria used to classify severity (and the value (i.e., 1-5)) of each hazard is found in the SMS Manual Table 4-2 [2] and is summarized below in Table 2-2. The severity of the worst credible effect for each of the identified hazards is presented in the hazard analysis worksheets in Appendix D.

Table 2-2: Safety Severity Categories

| | | |
|----------|-------------------------|---|
| 1 | Catastrophic | Results in multiple fatalities. |
| 2 | Hazardous | Reduces the capability of the system or the operator ability to cope with adverse conditions to the extent that there would be: (1) Large reduction in safety margin or functional capability (2) Crew physical distress/excessive workload such that operators cannot be relied upon to perform required tasks accurately or completely (3) Serious or fatal injury to small number of persons (other than flight crew) |
| 3 | Major | Reduces the capability of the system or the operators to cope with adverse operating condition to the extent that there would be – (1) Significant reduction in safety margin or functional capability (2) Significant increase in operator workload (3) Conditions impairing operator efficiency or creating significant discomfort (4) Physical distress to occupants of aircraft (except operator), including injuries Major occupational illness and/or major environmental damage, and/or major property damage |
| 4 | Minor | Does not significantly reduce system safety. Actions required by operators are well within their capabilities. Including: - (1) Slight reduction in safety margin or functional capabilities (2) Slight increase in workload such as routine flight plan changes (3) Some physical discomfort to occupants or aircraft (except operators) Minor occupational illness and/or minor environmental damage, and/or minor property damage |
| 5 | No Safety Effect | Has no effect on safety |

Next, existing controls in the NAS system were identified that either prevent or reduce the probability of the hazard occurring at all, or should the hazard occur, prevent or reduce the

likelihood of the worst credible severity effect from occurring. Existing controls can be requirements, equipage, procedures, and/or environmental conditions. Many of the existing controls are not specific to the NAS Communication System itself (e.g., the requirement to protect the airspace of both the current and amended clearance is a control of the NAS system as a whole). Existing controls were implemented specifically with safety in mind. Should any of the existing controls be deleted or modified, the NAS Communication System hazards must be re-assessed. The existing controls identified by the safety analysis are shown in

Table 2-3.

Table 2-3: Existing NAS Communication System Safety Controls

| | Existing Control |
|-----|---|
| 1. | The air-ground Terminal Communications (TCOM) and En Route Communications (ECOM) communication shall be in accordance with Communication Diversity Order 6000.36A |
| 2. | The NAS shall provide air-ground communications capabilities on a continuous basis. (NAS-SR-1000 3.6.1.E) |
| 3. | The air-ground communication system shall comply with Critical services performance requirements: Availability - 0.99999; No single point of failure of equipment, system, installation or facility shall cause loss of service to the user/specialist; The goal for a single loss of critical service to a user/specialist shall not exceed the duration of 6 seconds; The frequency of occurrence goal for any loss of service shall not exceed one per week. (NAS SR-1000 Section 3.8.1 <i>Operational Readiness</i> , Table 3.6.1). |
| 4. | The NAS shall provide specialists with the capability to communicate with aircraft and vehicles in the airport movement area. Alternative forms of communication, such as visual signals transmitted by specialists, shall be provided in case normal air-ground voice and data communications fail or are unavailable. (NAS-SR-1000 3.2.11.F) |
| 5. | The pilot in command of an aircraft is directly responsible for, and is the final authority as to, the operation of that aircraft. (FAA Order 7110.65 91.3(a)) |
| 6. | Standard no com procedures - Alternate control procedure (i.e., light gun instructions from towers) - “See and Avoid” procedures are prescribed. (Aeronautical Information Manual [AIM] 5-5-8 and Federal Aviation Regulations [FAR] 91.113) |
| 7. | Current separation standards. (FAA order 7110.65) |
| 8. | Procedures for maintaining clearance limits [definitions of clearance limit are FAA Pilot/Controller Glossary also the ICAO definition, ATC Clearance limit procedures are prescribed (7110.65, 4-6-1a Clearance Limit and FAR 91.185)] - ICAO PANS-RAC 4444: paragraph 5.2.1.1 “No clearance shall be given to execute any maneuver that would reduce the spacing between two aircraft to less than the separation minimum |
| 9. | Aircraft under radar and/or visual surveillance (except ocean and some ground environments in IMC). (FAA Order 7110.65P Effective Data August 4, 2005 Chapter 5 Radar and Visual p7-2-1.) |
| 10. | Aircraft-to-aircraft communications remains available (airborne or on-ground) |
| 11. | ATC procedures to transfer communication functions (after communication failure) to other positions/sectors/facilities are prescribed. (7110.65, 10-4-4) |
| 12. | Possible alternative communications capabilities (e.g., cell phone, public telephone, AOC, satellite phone when available relay (neighboring facility). Local SOP tailored to that facility and good operating procedures or FAA Order 7110.65P Effective Data August 4, 2005 Chapter 10 Emergencies section 1 General 10-1-1d. |
| 13. | TCAS is available for Transport Category Aircraft. (FAR 14CFR Part 129.18) |

| | Existing Control |
|-----|---|
| 14. | Procedures requiring “pilot acknowledgement/read back” when ATC issues clearances or instructions (7110.65, 2-4-3). |
| 15. | Controllers can also determine aircraft action through surveillance; IDENT, observing radar screen. (FAA Order 7110.65P Effective Data August 4, 2005 Chapter 5 Radar) |
| 16. | Controllers are required to order a clearance such that the critical information cannot be lost due to a failure truncating a message. |
| 17. | Air-to-air communications still available, so another aircrew may hear a step on or incorrect read-back and notify, and/or aircraft can announce intentions on party line |
| 18. | Procedures requiring aircraft identification for clearance (7110.65, 2-4-20) - Call sign/runway id (not shortened call sign) - Procedures for identification of the aircraft requesting clearances - Procedures for giving aircraft ID in granting clearances |
| 19. | Procedures requiring Facility Identification (7110.65, 2-4-8) for the ATC facility giving the clearances. |
| 20. | ICAO Annex 11: paragraph 3.5.1 “A controlled flight shall be under the control of only one air traffic control unit at any given time.” - The aircraft shall accept clearances/instructions only from the current control authority |
| 21. | The intended recipient is also listening so he/she may query or chime in (party line) |
| 22. | Voice procedures: - Procedures for giving aircraft ID in granting clearances - Procedures for communication when aircraft have same or similar call signs |
| 23. | Voice and data communications shall have the following response capabilities: --Initiation of one-way air-ground voice transmissions shall be possible within 250 milliseconds of keying the specialist’s microphone. --The ground-air transmission time for data messages shall not exceed 6 seconds. (NAS-SR-1000 3.6.1.A.5) |
| 24. | Time critical clearance can be sent with constraint (e.g. to reach by, cross at or before etc.). Thus if message was too late then aircrew would have send an UNABLE response. FAA Order 7110.65P (Chapter 4, Section 3 Departure Procedures 4-3-4 a. Clearance Void Times). |
| 25. | ADS report (surveillance) can provide aircraft position. (FAA Order 7110.65P Effective Data August 4, 2005 Chapter 5 Radar) |
| 26. | CPDLC pilot position reports can provide aircraft position |
| 27. | Oceanic separation standards. (FAA Order 7110.65P Effective Data August 4, 2005 Chapter 8 Offshore/Oceanic Procedures) |
| 28. | Clearly intelligible air-ground voice communications shall be provided. (NAS-SR-1000 3.6.1.A) |
| 29. | Procedures requiring Emphasis for Clarity (7110.65, 2-4-15) |
| 30. | Only one Pre-Departure Clearance (PDC) is sent (thus cannot get out of order) |
| 31. | Airport design minimizes runway and taxiway crossing by vehicles |
| 32. | Standard no com procedures |
| 33. | Vehicle operation training/ licensing for airport operations Part 139.329(e) requires that "each certificate holder shall -- ensure that each employee, tenant, or contractor who operates aground vehicle on any portion of the airport that has access to the movement area is familiar with the airport's procedures for the operation of ground vehicles and the consequences of noncompliance." To comply with Part 139.329(e), airport operators should have a ground vehicle guidebook for training personnel authorized to operate a ground vehicle on the airport. Part 139.301 Records – ground vehicle training; 139.303 Personnel Sufficient Qualified Personnel (303a), Properly Equipped (303b), Trained (303c), Record of Training for 24 CCM (303d) |

| | Existing Control |
|-----|--|
| 34. | Vehicles all yield to aircraft: AC 150/5210-20 Ground Vehicle Operations on Airports - guidance to airport operators in developing training programs for safe ground vehicle operations, Sample Ground Vehicle Operations Training Manual Appendix B 1.7.10. No vehicle operator shall enter the movement area— <ul style="list-style-type: none"> a. Without first obtaining permission of the (AIRPORT OPERATOR) and clearance from the ATCT to enter the movement area; b. Unless equipped with an operable two-way radio in communication with the ATCT; or c. Unless escorted by an (AIRPORT OPERATOR) vehicle and as long as the vehicle remains under the control of the escort vehicle. |
| 35. | Vehicles under visual surveillance or radar/multi-lateration surveillance: FAA Order 7110.65, Air Traffic Control Handbook, paragraph 3-1-3, "Use of Active Runways," states, "The local controller has primary responsibility for operations conducted on the active runway and must control the use of those runways." Paragraph 3-1-12, "Visually Scanning Runways," states that, "Local controllers shall visually scan runways to the maximum extent possible." |
| 36. | Mobile-to mobile communications still available |
| 37. | The NAS shall provide specialists with the capability to communicate with aircraft and vehicles in the airport movement area. Alternative forms of communication, such as visual signals transmitted by specialists, shall be provided in case normal air-ground voice and data communications fail or are unavailable. (NAS-SR-1000 3.2.11.F) |
| 38. | Possible alternative communications capabilities e.g., cell phone, ATCT light gun procedures |
| 39. | Title 14, Code of Federal Regulations (CFR), Part 139 (14 CFR Part 139] requirement to familiarize vehicles for operating on a given airport. |
| 40. | FAA Order 7110.65, Air Traffic Control Handbook, paragraph 3-1-3, Use of Active Runways, - The local controller has primary responsibility for operations conducted on the active runway and must control the use of those runways. |
| 41. | AC 150/5340-18D Standards for Airport Sign Systems Part 139.311 CFR MARKING, SIGNS AND LIGHTING AC 150/5210-22 Airport Certification Manual (ACM): Paragraph 302(a) "Airport sign and marking plans must receive FAA approval before they are implemented" Chapter 5. Section 139.311 "Include in the ACM a legible color diagram of the airport sign and marking systems." |
| 42. | FAA Order 7110.65 Paragraph 3-1-12, Visually Scanning Runways - Local controllers shall visually scan runways to the maximum extent possible. |
| 43. | CFR Part 139.329(b) airport operators are required to establish and implement procedures for operation of ground vehicles in the safety area as well as the movement area. |
| 44. | CFR Part 139.205(b)(19) requires that these procedures be included in the Airport Certification Manual (ACM). |
| 45. | Controller use of full call sign/runway ID (not shortened) (FAA Order 7110.65P 3-7-1 Ground Traffic Movement <i>Phraseology</i>) |
| 46. | Controllers must establish position before moving vehicle (FAA Order 7110.65 Section 1 General 3-1-7 Position Determination) |
| 47. | Procedures for identification of vehicles requesting clearances (Part 139CFR ground vehicle guidebook for training) |
| 48. | Controller procedures for giving vehicle ID in granting clearances (FAA Order 7110.65 Section 7 Taxi and Ground Movement Procedures 3-7-2 Taxi and Ground Movement Operations) |
| 49. | Vehicle readback procedures (voice) (Part 139CFR ground vehicle guidebook for training) |
| 50. | Intrafacility communication requirements have been minimized due to automation of many functions |

| | Existing Control |
|-----|---|
| 51. | Controller/ assistant/ supervisor can walk over and talk to other controller. |
| 52. | Voice messages would not get a proper acknowledgement, when truncated due to a failure (Procedure between interphone intra/interfacility communication which utilize numeric position identification, the caller must identify both position and facility (FAA Order 7110.65P 2-4-12 Interphone Message Format) e. The receiver states the response to the caller's message followed by the receiver's operating initials. f. The caller states his or her operating initials). |
| 53. | SR-1000: 3.6.2A 1: The NAS shall provide direct-access voice communications connectivity between specialist in on ATC facility and designated specialist in another facility as shown in Table 3-1. The number of direct-access calls that are blocked because of saturation of equipment shall not exceed 1 in 1000 calls. |
| 54. | Other facility can be reached by other means (Local Contingency Plan - FAA Order 7210.3 Facility 2-1-7 Air Traffic Service (ATS) Continuity a. Facilities shall develop and maintain current operational plans and procedures to provide continuity of required services during emergency conditions (e.g. power failures, fire, flood) b. Contingency plans). <ul style="list-style-type: none"> · Relay through aircraft · Cell phones · Public phone system (FAA Order 7210.3 Section 3, 3-3-1. SERVICE "F" COMMUNICATIONS Facility AT managers shall establish procedures to provide interim communications in the event that local or long-line standard Service "F" fail. These shall include the use of telephone conference circuits and the use of airline or other facilities;;3-3-2. TELEPHONE COMMUNICATIONS) |
| 55. | Facilities periodically check availability of communications with other facilities and would be aware of loss of communications. |
| 56. | Procedures exist to transfer control to another facility in case of failure. (e.g. primarily redundancy: ARTCC to ARTCC and ARTCC to Command Center rely through third party) FAA Order 7210.3 Facility Operation and Administration; Section 3. Letters of Agreement (LOA) 4-3-1. LETTERS OF AGREEMENT ;4-3-2. APPROPRIATE SUBJECTS Examples of subjects of LOAs are: a. Between ARTCCs: 1. Radar handoff procedures.2. Interfacility coordination procedures.3. Delegation of responsibility for IFR control jurisdiction |
| 57. | Procedures exist to have aircraft initiate transfer with receiving facility. (FAA Order 7110.65P 8-2-2 Transfer of Control and Communications). |
| 58. | Automation and visual alerts to detect: <ul style="list-style-type: none"> - Aircraft positions - Out-of-conformance - Potential conflicts |
| 59. | 7110: IFR operations in any class of controlled airspace, a pilot must receive an appropriate ATC clearance prior to entering in the airspace. |
| 60. | Inter-facility data communications shall be provided with error detection and correction capabilities (NASSRS 3.6.3.A.11) NAS systems digital circuits basic requirement to provide in excess of 99.9% error free seconds. |
| 61. | NAS-SR-1000 p3.6.2.A.3 Ground-Ground Interfacility Communications Connectivity 5) Clearly intelligible interfacility voice communications shall be provided. |
| 62. | FTI Attachment J.1, FAA Telecommunications Services Description (FTSD): Voice Quality Mean Opinion Score (MOS) equal to or greater than 4.3. |
| 63. | ATC uses judgment whether or not to clear aircraft to land. (FAA Order 7110.65P 3-1-5. <u>VEHICLES/EQUIPMENT/ PERSONNEL ON RUNWAYS</u>) |
| 64. | The NAS shall provide the specialist with an unobstructed view of the airport movement area. (NAS-SR-1000 3.2.11.D). |

| | Existing Control |
|-----|---|
| 65. | The NAS shall be capable of continuously broadcasting the latest approved aerodrome and terminal area conditions on communications media which can be accessed by aircraft in flight and on the ground. (NAS-SR-1000 3.3.3.B). |
| 66. | Aeronautical information shall be continuously (24 hours a day) accessible to specialists. (NAS-SR-1000 3.1.2.B). |
| 67. | Aeronautical information shall be continuously (24 hours a day) accessible to users upon request with or without the aid of specialists. (NAS-SR-1000 3.1.2.C). |
| 68. | Aeronautical information shall be obtainable along a specified route, or in conjunction with specified locations or areas, or by reporting location. (NAS-SR-1000 3.1.2.D). |
| 69. | Real-time required communication between FIRs has been minimized; most transfers can be done sufficiently in advance. (FAA Order 7110.65P Section 8-2-1 <u>Coordination</u>) |
| 70. | Foreign ATC can be reached by other means: <ul style="list-style-type: none"> • Relay through aircraft • Cell phones • Public phone system |
| 71. | In a two-way exchange; usually getting cut-off etc. would be detected by one or both parties and coordination would be attempted again; it would be rare for the failure to go undetected. |
| 72. | Boundary Coordination Times are agreed by Memorandum of Understanding between FIRs. (FAA Order 7110.65P 8-2-2) |
| 73. | Receiving ground system has flight plan. (FAA Order 7110.65P 8-2-1 a) |
| 74. | Receiving ground system would initiate coordination/transfer. (FAA Order 7110.65P 8-2-2) |
| 75. | ICAO format boundary coordination messages are tagged and time stamped. |
| 76. | AOC-ATC messages cannot affect separation. |
| 77. | Aircraft have highly reliable systems. (AC-25-11 viii, Loss of all communication functions must be improbable; RTCA/DO-254 Design Assurance Guidance for Airborne Electronic Hardware; AC 25.1309-1A (Air Transport) SYSTEM DESIGN AND ANALYSIS; AC 23.1309-1C (General Aviation) EQUIPMENT, SYSTEMS, AND INSTALLATIONS IN PART 23 AIRPLANES;FAA FAR 121 requirement of "two means of communication for the intended operating environment") |
| 78. | Standard operating procedures/pilot training |
| 79. | Redundancy to prevent interruption - centers can talk to multiple facilities (2 or 3 facilities typical) and command center |
| 80. | Diverse entry points into facilities. (Communication Diversity Order 6000.36 A). |
| 81. | Procedure to switch to emergency operational AT procedures. (FAA Order 7210.3 Facility Operation and Administration Section 3 Letters of Agreement (LOA) 4-3-1 Letters of Agreement; g. Establish responsibilities for: 2. Providing emergency services). |
| 82. | Procedure to switch to FAA-owned communications systems – FAATSAT transportable equip., RCL, portable air-ground radio. |
| 83. | IDAT parity and checksum to reliably detect corruption of the message. |

Next, the likelihood of the occurrence of given hazard that then in turn results worst credible affect was assessed. This assessment was done by reviewing available data on accidents and incidents in the NAS and using subject matter expertise of the probability the worst credible effect occurring. However, for an identified hazard, this safety analysis considers hazard causes to be limited to NAS Communication System failures. When reviewing available data, specific causes were not

necessarily identified. The criteria used to classify likelihood (and the value (i.e., A-E)) of the safety hazards is found in the SMS Manual Table 4-2 [2] and is summarized below in

Table 2-4. The likelihood of occurrence of the worst credible effect for each of the identified hazards is presented in the hazard analysis worksheets in Appendix D.

Table 2-4: Safety Likelihood Categories

| | | |
|----------|-----------------------------|--|
| A | Frequent | Qualitative: Anticipated to occur one every three months during the operational life of an item Quantitative: Probability of occurrence per operational hour is equal to or greater than 1×10^{-3} |
| B | Probable | Qualitative: Anticipated to occur one or more times during the entire system/operational life of an item Quantitative: Probability of occurrence per operational hour is equal to or greater than 1×10^{-5} |
| C | Remote | Qualitative: Unlikely to occur to each item during its total life. May occur several time in the life of an entire system or fleet Quantitative: Probability of occurrence per operational hour is less than 1×10^{-5} , but greater than 1×10^{-7} |
| D | Extremely Remote | Qualitative: Not anticipated to occur to each item during its total life. May occur a few times in the life of an entire system or fleet Quantitative: Probability of occurrence per operational hour is less than 1×10^{-7} , but greater than 1×10^{-9} |
| E | Extremely Improbable | Qualitative: So unlikely that it is not anticipated to occur during the entire operational life of an entire system or fleet Quantitative: Probability of occurrence per operational hour is less than 1×10^{-9} |

Finally, risk was determined for each NAS Communication System hazard using its severity and likelihood values based on Figure 4-7 of the SMS Manual [2] and shown below in Figure 2-2.

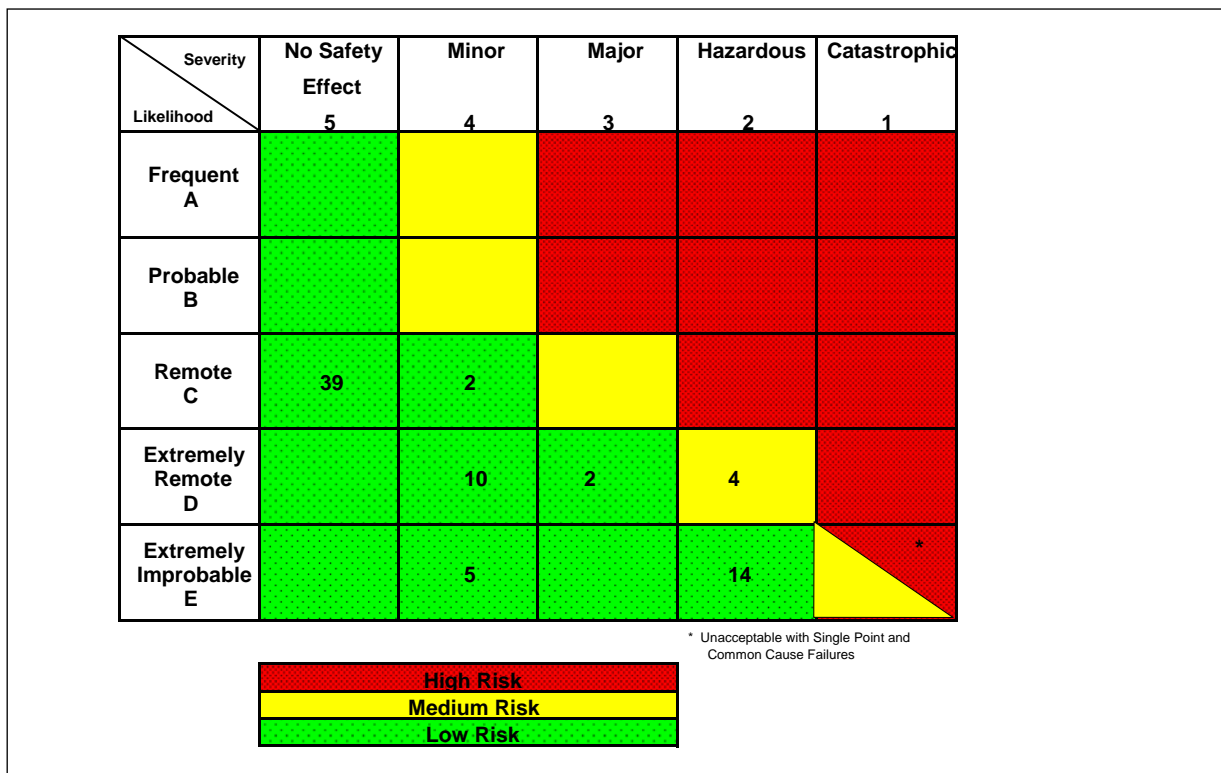


Figure 2-2: Predictive Risk Matrix

A summary of the risk associated with each of the 120 hazards identified for the NAS Communication System is shown in Table 2-5 and detailed in the hazard worksheets in Appendix D.

Table 2-5: NAS Communication System Safety Risk Summary

| Hazard Category | 1. ATC-Aircraft | 2. ATC Vehicle | 3. Intrafacility | 4. Interfacility | 5 NAS-OGA | 6. NAS-Foreign | 7. NAS-AOC | 8. Aircraft-Aircraft⁴ | 9 Aircraft/Vehicle¹ |
|------------------------------------|------------------------|-----------------------|-------------------------|-------------------------|------------------|-----------------------|-------------------|---|---------------------------------------|
| 1. NAS Total Unav | 3D | 4E | 5 | 4D | 2E | 4D | 5 | 4E | N/A |
| 2. NAS Partial Unav | 3D | 4E | 5 | 4D | 2E | 4D | 5 | 4E | N/A |
| 3. NON NAS Unav | 4D | 4D | N/A | N/A | N/A | N/A | N/A | 4D | N/A |
| 4. Single Recipient Failure | 4C | 4D | 2E | 2E | 2E | 2E | 5 | 5 | N/A |
| 5. Multiple Recipient Failure | 4C | 4E | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 6. NOT Control Auth Separation | 2D | 2E | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 7. NOT Control Auth NOT Sep | 5 | 5 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 8. Unintended Recipient Separation | 2D | 2E | 5 | 5 | 5 | 5 | N/A | NC ³ | N/A |
| 9. Unintended Recipient NOT Sep | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | N/A |
| 10. Late Separation | 2D | N/A | N/A | 5 | NC ³ | 5 | N/A | N/A | N/A |
| 11. Late NOT Sep | 5 | N/A | N/A | 5 | NC ³ | 5 | 5 | N/A | N/A |
| 12. Corruption Separation | 2D | 2E | 2E | 2E | 2E | 2E | N/A | 2E | N/A |
| 13. Corruption NOT Sep | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | N/A |
| 14. Out of Sequence Separation | 4D | N/A | N/A | 5 | NC ³ | 4D | N/A | N/A | N/A |

| Hazard Category | 1. ATC-Aircraft | 2. ATC Vehicle | 3. Intrafacility | 4. Interfacility | 5 NAS-OGA | 6. NAS-Foreign | 7. NAS-AOC | 8. Aircraft-Aircraft ⁴ | 9 Aircraft/Vehicle ¹ |
|-----------------------------|-----------------|----------------|------------------|------------------|-----------------|----------------|------------|-----------------------------------|---------------------------------|
| 15. Out of Sequence NOT Sep | 5 | N/A | N/A | 5 | NC ³ | 5 | 5 | N/A | N/A |

Table Notes:

1. No NAS ATS messages have been identified, so N/A.
2. Where a hazard was split into two cases, the most significant risk is shown
3. NC- No credible scenario having a safety effect was envisioned.
4. Aircraft-aircraft hazards are all consider second level failures. This only applies when NAS ATS-aircraft communications have failed.

The detailed results are presented in the worksheets in Appendix D. In summary, the 120 hazards identified in functional categories 1-8 breakdown as follows:

- High risk – 0 (none) hazards.
- Medium risk – 4 hazards
- Low risk – 72 hazards
- N/A or NC 44 hazards

2.2.4 Assessing NAS Communication System Safety Risks

The fourth step in the safety analysis is to assess the risk. None of the hazards associated with the existing NAS Communication System were determined to be high risk. Since none of the hazards were found to be high risk, no treatment of any identified risk has been identified.

2.2.5 Treating NAS Communication System Safety Risks

The final step in the safety analysis is to treat the risk. The current NAS communication system has been declared safe. This analysis did not identify any requirements beyond the existing controls.

2.3 Safety Analysis Conclusions

The SSTF performed a safety hazard analysis in order to provide a safety baseline for the existing NAS Communication System.

The NAS Communication System safety assessment was performed SMS compliant. No recommended requirements were identified.

Procedural conclusions: The safety hazard analysis was coordinated with the security threat analysis described in Section 3. In particular:

- A common functional breakdown of the system was used as a starting point for both the safety and security analyses.
- Any recommended requirements were coordinated to ensure that a minimal set of requirements was introduced, and that new safety requirements had no adverse effect on security and vice versa. (This turned out to be not necessary since neither safety nor security identified any definitive new requirements.)

Technical conclusions: No hazards, with an unacceptable risk, were identified during the safety analysis. However a number of hazards with a medium risk were identified. Furthermore, it must

be emphasized that this effort represented only a high-level safety hazard analysis it is recommended that detailed, safety hazards analyses be performed as a follow-on activity to assess particular components of the NAS Communication System.

3 Security Threat Analysis

This section discusses the security threat analysis that was performed on the existing NAS Communication System.

3.1 NAS Communication System Security Analysis Process

Information security concerns the protection and defense of information and information systems. The purpose of information security is to ensure confidentiality, integrity, and availability of information in the face of deliberate attacks. Here confidentiality, integrity, and availability are defined in a security context as follows:

- **Confidentiality:** Assurance that information is not disclosed to unauthorized persons, processes, or devices.
- **Integrity:** Assurance that an information system is operating without unauthorized modification, alteration, impairment, or destruction of any of its components.
- **Availability:** Assurance that information and communications services will be ready for use when expected.

Integrity and availability have established definitions in the aeronautical community, however their usage in a security context is subtly different. Specifically, integrity and availability in an aeronautical context are typically focused on providing assurance in the face of accidental errors, whereas, in a security context they are focused primarily on providing assurance in the face of deliberate attacks.

It is instructive to compare information security with safety – a discipline which is well-established in the aeronautical community. The key distinction is that traditionally safety has been concerned with the prevention of accidental errors and failures while information security focuses on deliberate attacks. This implies that information security is evolutionary, since the capabilities and motivations of attackers change over time.

The evolutionary nature of information security means that it is important to follow a defined process during security threat analysis of systems so that the motivation for requirements is well-understood and the analysis can be revisited and revised as attacks change. The process used to analyze security threats to the existing NAS Communication System is summarized in Figure 3-1.

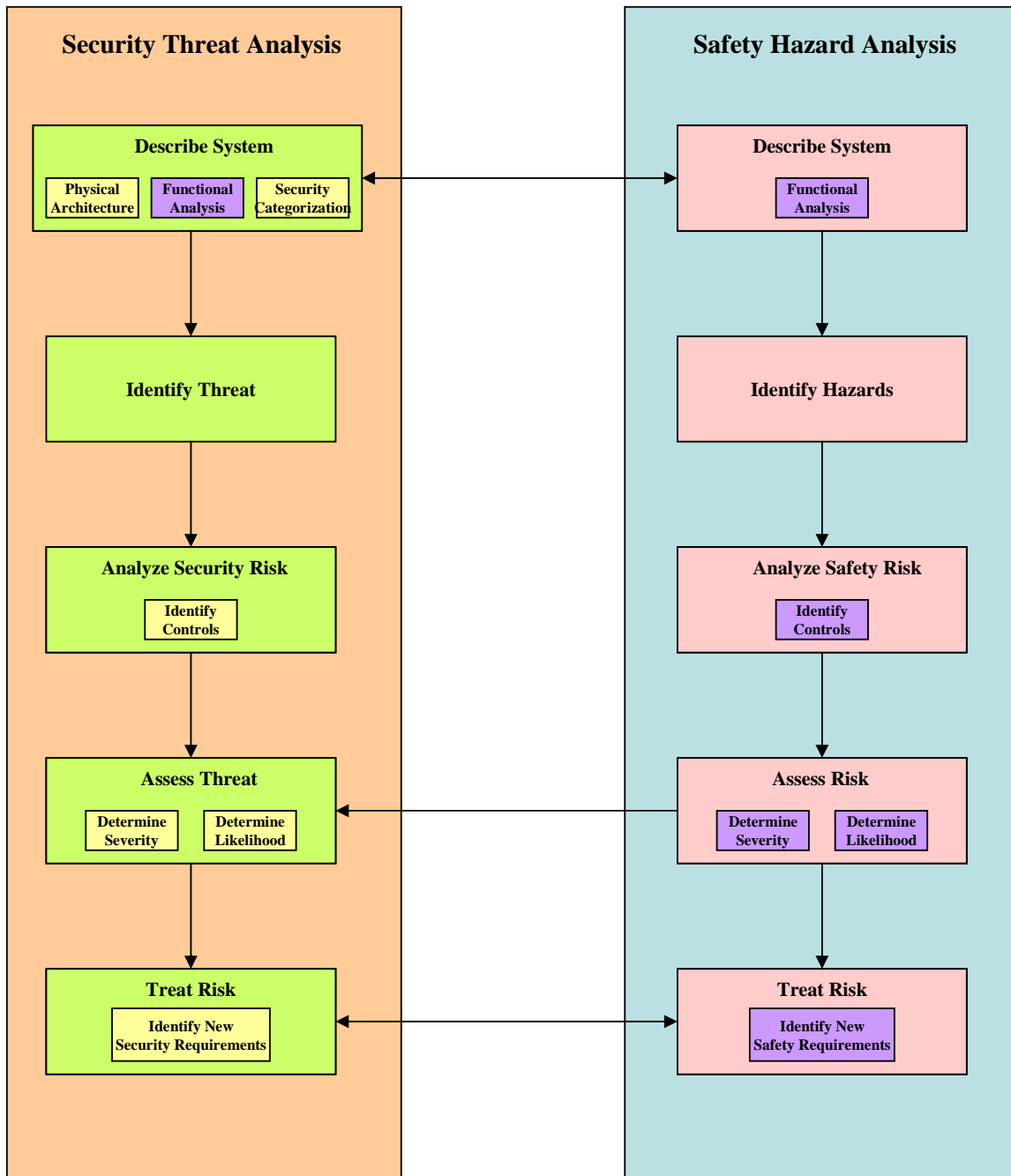


Figure 3-1: The Security Threat Analysis Process

The security threat analysis process shown in Figure 3-1 is adapted from the FAA’s SCAP [12] and NIST’s FISMA standards [13]. Adjustments were made to accommodate the desire to align the security threat analysis process as much as possible with the safety process, and to account for the high-level, rather than component-level nature of the study.

The process begins with asset identification, which provides the system’s architecture and aims to develop an understanding of the information types that the system handles. In

this case a functional analysis and a physical architecture were described. The activities are summarized in Section 1.5 and detailed in Appendices A and C respectively.

***Note:** In the context of this study, the same functional analysis and physical architecture descriptions were used as a starting point by both safety and security in order to maximize commonality between the two disciplines.*

The next step, security categorization, provides an initial assessment of the intrinsic sensitivity of the information being handled by the system in terms of confidentiality, integrity, and availability. Security categorization that was performed here is summarized in Appendix E.

Next, the risk/threat analysis examines the threats to the system. The high-level threats to the system are identified, focusing on areas that have been shown to be likely concerns based on the security categorization. Then the severity and likelihood of the threats is assessed in light of the existing security controls. In this case the safety hazard analysis was used to determine threat severity by determining which hazards each threat may cause and then assigning the threat severity level based on the relevant hazard classes. The goal of risk analysis is to determine whether the existing risk to the system is acceptable or not. The risk assessment performed here is summarized in Sections 3.2.1 and 3.2.2, and detailed in Appendix F.

Finally, if the risk analysis has determined that some threats are not sufficiently mitigated, then new security requirements and recommendations are developed to address the threats. Any new requirements are coordinated with safety in order to ensure that new security requirements do not result in new safety hazards and vice versa. In some cases new requirements from safety and security can also be harmonized to avoid duplication. Any new security requirements identified here are discussed in Section 3.2.3.

Both security categorization and risk analysis require impact/severity rankings. “High/medium/low” rankings are common in security circles, but here slightly different rankings have been adopted. Specifically “none”, “low”, “medium”, “high – severe”, and “high – catastrophic” are used. These categories roughly correspond to the standard safety hazard classes “no safety effect”, “minor”, “major”, “hazardous”, and “catastrophic” respectively, although in general security considers financial impact, impact on public perception, and the like in addition to safety-related impact. The detailed definitions for the categories are provided in Table 3-1.

Table 3-1: Security Severity Categories

| Severity Category | Definition |
|-------------------|---|
| None | Safety – General: no or negligible safety impact. Air traffic control: slight increase in ATC workload. Flying public: inconvenience. Corresponding hazard class: 5 (No Safety Effect). |
| | Availability – No impact. |
| | Cost – No financial loss. |
| | Passenger Privacy - No impact. |
| | Exposure of Proprietary Information: No impact. |

| Severity Category | Definition |
|----------------------|---|
| | Public Perception - No impact. |
| Low | <p>Safety - General: limited safety impact, includes self-repairing and limited damage or disruption to system functions. Air traffic control: degradation in mission capability to an extent and duration that the current NAS Communication System is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; or significant increase in ATC workload. Flying public: slight increase in flight crew workload, or slight reduction in safety margin or functional capabilities, or minor illness or damage, or some physical discomfort. Corresponding hazard class: 4 (Minor)</p> |
| | Availability - Recoverable loss of redundancy or backup capability. |
| | Cost – Minor financial loss, or minor damage to assets |
| | Passenger Privacy - Exposure of limited private information of small number of people. |
| | Exposure of Proprietary Information: Disclosure of non-sensitive airline operation information. |
| | Public Perception – Distrust of some passengers in aircraft. |
| | |
| Medium | <p>Safety - General: serious safety impact. Example: system failure, damage or disruption that impairs the safe control of air traffic over time and/or requires local restoration of systems capabilities. Air traffic control: significant degradation in mission capability to an extent and duration that the current NAS Communication System is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; or reduction in separation as defined by a low/moderate severity operational error, or significant reduction in ATC capability; or significant damage to current NAS Communication System assets. Flying public: significant increase in flight crew workload, or significant reduction in safety margin or functional capability, major illness, injury, damage, or physical distress. Corresponding hazard class: 3 (Major)</p> |
| | Availability – Significant flight delays. |
| | Cost - Significant financial loss, or Significant damage to assets. |
| | Passenger Privacy – Exposure of private information of small number of people. |
| | Exposure of Proprietary Information – Disclosure of some sensitive airline operation information. |
| | Public Perception - Strong distrust of some passengers in aircraft. |
| | |
| High - Severe | <p>Safety - General: severe safety impact. Example: system failure, damage or disruption that immediately affects the safe control of aircraft or destroys system assets beyond recovery capabilities. Air traffic control: severe degradation in, or loss of, mission capability to an extent and duration that the current NAS Communication System is not able to perform one or more of its primary functions; or reduction in separation as defined by a high severity operational error, or a total loss of ATC. Flying Public: large reduction in safety margin or functional capability, serious or fatal injury to small number , or physical distress/ excessive workload. Corresponding hazard class: 2 (Hazardous)</p> |
| | Availability – Flight interruptions. |
| | Cost – Major financial loss or severe damage to assets. |
| | Passenger Privacy – Exposure of private information of large number of people. |
| | Exposure of Proprietary Information - Disclosure of lots of sensitive airline operation information, some security information. |
| | |

| Severity Category | Definition |
|----------------------------|--|
| | Public Perception: Strong distrust of many passengers in aircraft. |
| High - Catastrophic | Safety - General: catastrophic safety impact, or total loss of systems control. Air traffic control: collision with other aircraft, obstacles, or terrain. Flying public: hull loss, multiple fatalities. Corresponding hazard class: 1 (Catastrophic) |
| | Availability – Fleet re-route. |
| | Cost – Huge financial cost, or destruction of aircraft. |
| | Passenger Privacy – Exposure of private information of large number of people. |
| | Exposure of Proprietary Information: Disclosure of highly sensitive airline operation information, security information. |
| | Public Perception: Complete distrust of many passengers in air traffic. |

The definitions of categories in Table 3-1 above are designed to maximize the commonality with established safety terminology. The definitions are derived from a number of sources: the FAA’s Information Systems Security Program Handbook [12], the FAA’s SSMP handbook [1], NIST Federal Information Processing Standards (FIPS) 199 [14], NIST Special Publication (SP) 800-30 [15], and the European Union’s Security of Aircraft in the Future European Environment (SAFE) project [16].

***Note:** The “None” and “Low” categories shown in Table 3-1 map to FIPS 199 “Low”. The “Medium” category shown in Table 3-1 maps to FIPS 199 “Medium”. The “High – Severe” and “High – Catastrophic” shown in Table 3-1 map to FIPS 199 High*

Risk analysis also requires threat likelihood rankings. Since a variety of different definitions are used in security circles and the desire in this case was to align with safety, here the safety likelihood rankings from

Table 2-4 are used. These rankings are given in Table 3-2. Note that security only makes use of the qualitative versions of the safety likelihood rankings since the presence of an attacker makes threat likelihood estimation considerably less precise than traditional safety hazard likelihood assessment.

Table 3-2: Security Likelihood Categories

| | |
|-----------------------------|---|
| Frequent | Anticipated to occur one every three months during the operational life of an item. |
| Probable | Anticipated to occur one or more times during the entire system/operational life of an item |
| Remote | Unlikely to occur to each item during its total life. May occur several time in the life of an entire system or fleet |
| Extremely Remote | Not anticipated to occur to each item during its total life. May occur a few times in the life of an entire system or fleet |
| Extremely Improbable | So unlikely that it is not anticipated to occur during the entire operational life of an entire system or fleet |

Finally, the security process needs to determine guidelines that can be used to decide, based on threat severity and threat likelihood, whether or not a particular threat represents an unacceptable risk. Figure 2-2 was adapted from the safety process for use by security

in order to maximize the commonality between the processes. Whether or not a threat was considered acceptable or not was based on Table 3-3 below.

Table 3-3: Security Risk Assessment Matrix

| Severity \ Likelihood | None | Low | Medium | High - Severe | High - Catastrophic |
|-----------------------|------|-----|--------|---------------|---------------------|
| Frequent | | | | | |
| Probable | | | | | |
| Remote | | | | | |
| Extremely Remote | | | | | |
| Extremely Improbable | | | | | |

In Table 3-3, a dotted green cell indicates a likelihood-severity pair that represents an acceptable risk, a more densely dotted red cell indicates a likelihood-severity pair that represents an unacceptable risk requiring further mitigation, and a solid yellow cell indicates a likelihood-severity pair that represents a moderate risk that may require additional analysis to determine if mitigation is recommended.

3.2 Security Analysis

This section summarizes the results of the security threat analysis. Further information on the analysis is in Appendices E and F.

Note: Due to the sensitivity of the information contained in Appendix F, this appendix will not be widely distributed. Contact the Security Team Lead for the ATC Communications Services Air-Ground Solution Development Group to request a copy of Appendix F.

3.2.1 Threat Identification

This section details the 41 high-level threats to the existing NAS Communication System that have been identified.

A major concern during threat identification is how to ensure that the threat list is complete. Many of the most effective attacks against systems, exploit threats that were simply not considered during system design and analysis.

To minimize the possibility of missed threats, the threat identification process used here has been “systematized” as follows:

- The threats are developed from existing threats lists to avoid “re-inventing the wheel”. In particular the NIST Commercial Off-The-Shelf (COTS) Protection Profiles (PP) [17] and the Future Communications System – Information Systems Security Architecture (FCS-ISSA) [18] were used as sources.
- The threats are listed in categories using a tree-like structure so that similar threats are grouped together.

During threat identification, attention was focused on communications threats associated with deliberate attacks. The focus on communications threats is consistent with the goals of the end-to-end analysis effort. The focus on threats associated with deliberate attacks rather threats associated with accidents and errors acknowledges that the existing safety process already adequately addresses accidents and errors.

***Note:** Threats associated with accidents and errors that enable deliberate attacks – which are common problems in practice – are considered in scope.*

The 41 threats identified for the existing NAS Communication System are listed in Table 3-4. Table 3-4 provides a comprehensive list of high-level threats. The inclusion of a threat in Table 3-4 does not imply that the threat requires mitigation.

Table 3-4: Security Threats to Existing NAS Communication System

| Threat Identifier | Threat Description |
|------------------------|---|
| T.ACCESS | An authorized user may gain unauthorized access via technical or non-technical attack for malicious or non-malicious purposes. |
| T.ACCESS.DISABLE | User deliberately disables or modifies security function in order to enable other attacks. |
| T.ACCESS.EAVESDROP | An authorized user eavesdrops messages which they are not authorized to read on a communications link in order to reduce the confidentiality of the system. |
| T.ACCESS.OTHER-TYPE | End user masquerades as another type of end user to deceive other users of the system. |
| T.ACCESS.SAME-TYPE | End user masquerades as another end user of the same type to deceive other users of the system. |
| T.ACCESS.TECHNICIAN | Technician masquerades as end user of the system in order to deceive users of the system. |
| T.DENIAL | System resources may become exhausted due to system error, non-malicious user actions, or denial-of-service (DoS) attack. |
| T.DENIAL.DISRUPT | An attacker disrupts a communications link in order to reduce the availability of the system – e.g., by unplugging or severing cables. |
| T.DENIAL.FLOOD | An attacker floods a communications link with injected messages in order to reduce the availability of the system. |
| T.DENIAL.JAM | An attacker jams packets on a Radio Frequency (RF) communication link in order to reduce the availability of the system. |
| T.DENIAL.MALFORM | An attacker injects malformed messages into a communications link in order to reduce the availability of the system. |
| T.DEVELOP | Security failures may occur as the result of problems introduced during design, development, and implementation of the system. |
| T.DEVELOP.CM | Poor configuration management during implementation results in deployment of incorrect, insecure system. |
| T.DEVELOP.FLAW | Security flaw accidentally inserted into system during implementation by authorized individual. |
| T.DEVELOP.IMPLEMENT | System security requirements not implemented as specified. |
| T.DEVELOP.REQUIREMENTS | System security requirements do not adequately address identified threats and vulnerabilities. |
| T.DEVELOP.THREATS | Threat analysis is not adequate – important threats not considered or threat severity and likelihood incorrectly estimated. |

| Threat Identifier | Threat Description |
|------------------------|---|
| T.DEVELOP.TRAPDOOR | Security flaw or trapdoor deliberately inserted into system during implementation by authorized or unauthorized individual. |
| T.ENTRY | An individual other than an authorized user may gain access via technical or non-technical attack for malicious purposes. |
| T.ENTRY.ALTER | An attacker delays/deletes/injects/modifies/re-directs/re-orders/replays or otherwise alters messages on a communications link in order to reduce the integrity of the system. |
| T.ENTRY.EAVESDROP | An attacker eavesdrops messages on a communications link in order to reduce the confidentiality of the system. |
| T.ENTRY.IMPERSONATE | An attacker impersonates a user of the system in order to reduce the confidentiality or integrity of the system. |
| T.ENTRY.MALFORM | An attacker injects malformed messages into a communications link in order to gain control of a system component and indirectly reduce the integrity of the system – e.g., buffer overflow attack. |
| T.ENTRY.SOFTWARE | An authorized user may introduce unauthorized software (malicious or otherwise) into a system and compromise the integrity and availability of information |
| T.FAILURE | The secure state of the system could be compromised in the event of a system failure. |
| T.FAILURE.DENIAL | System loses security configuration information during failure and as a result is unable to re-establish communications upon re-start resulting in denial-of service. |
| T.FAILURE.DISABLE | System recovers from failure by re-initializing with security function disabled. |
| T.FAILURE.FALLBACK | System enables use of security credentials which have previously been compromised during failure recovery. |
| T.FAILURE.LOG | System compromises security information by writing to unprotected log during failure. |
| T.INSTALL | The system may be delivered or installed in a manner that undermines security. |
| T.INSTALL.COMPROMISE | Security credentials stored on system compromised during delivery. |
| T.INSTALL.DISABLE | System incorrectly installed so that security functions are not enabled. |
| T.INSTALL.INCORRECT | Incorrect security parameters established during system installation resulting in security weakness. |
| T.MAINTAIN | The security of the system may be reduced or defeated due to errors or omissions in the administration and maintenance of the system. |
| T.MAINTAIN.ACCIDENTAL | Security accidentally circumvented by technician – e.g., due to lack of training. |
| T.MAINTAIN.DELIBERATE | Security deliberately circumvented by technician – e.g., because security is so cumbersome that effective maintenance is not possible otherwise. |
| T.MAINTAIN.KEY-MANAGE | Security compromised due to poor management of security credentials. |
| T.MAINTAIN.LOG-REVIEW | Security problem is undetected because security logs are not reviewed regularly and thoroughly. |
| T.MAINTAIN.PATCH | Security compromised because flaws are identified in the system, but patches are not developed and deployed in a timely manner. |
| T.OBSERVE | Events occur in system operation that compromise security, but the system, due to flaws in its specification, design, or implementation, may lead a competent user or technician to believe that the system is still secure. |
| T.OBSERVE.LOG-OVERKILL | Security compromise undetected because too much log information collected and administrator is unable to identify most serious problems. |
| T.OBSERVE.LOG-PROTECT | Security compromise undetected because attacker is able to modify or destroy alarm and log before they reach user or technician. |
| T.OBSERVE.REPORT | Security compromise undetected due to poor reporting of security events. |
| T.OBSERVE.UNABLE | Security compromise undetected because the system is unable to detect problem – for example unable to detect physical connection being broken. |
| T.OPERATE | Security failures may occur because of improper operation of the system. |
| T.OPERATE.ACCIDENTAL | Security accidentally circumvented by user – e.g., due to lack of training. |
| T.OPERATE.DELIBERATE | Security deliberately circumvented by user – e.g., because security is so cumbersome that effective operation is not possible otherwise. |
| T.PHYSICAL | Security-critical parts of the system may be subjected to a physical attack that may compromise security. |
| T.PHYSICAL.COMPROMISE | Security credentials (e.g., cryptographic keys) stored by system are compromised by physical attack. |
| T.PHYSICAL.DENIAL | System physically damaged, resulting in DoS attack. |
| T.TRACEABLE | Security relevant events may not be traceable to the user or process associated with the event. |
| T.TRACEABLE.UNABLE | Security compromise detected but unable to identify user or process associated with the event due to lack of log information. |

3.2.2 Existing NAS Communication System Security Controls

The NAS Communication System has a wide array of existing technical, managerial and operational security controls. The list of existing security controls in this section represents a summary and is not comprehensive. Only those controls which are either common to several NAS sub-systems and/or mitigate significant threats are included in this section. A more detailed list is included in Appendix F.

Many of the existing security controls were not implemented specifically with security in mind. Rather they are characteristics of the system which happen to help address security threats. Availability of time did not allow for a comprehensive investigation of how the existing security controls are implemented. Without interviewing personnel involved and assessing fielded systems, information about how security controls are effective is difficult to present. Instead, the analysis focused on the supported capabilities. How the capabilities are used is fundamental to the security of the system and an assessment of how the controls are used would be a valuable follow-on task.

A comprehensive evaluation of all fielded components was not performed. The analysis only focused on identifying pervasive trends. For example: several voice switch sub-systems were investigated and found to support access control for Monitoring, Maintenance, and Control (MMC) activities. This does not imply that all voice switches support access control for MMC. Similarly, many sub-systems support identification and authentication based on usernames and passwords. This does not imply that all these sub-systems implement passwords securely. An attacker is likely to seek out the weakest link in a system and thus detailed assessment of all controls and all components would be a valuable follow-on task

Existing security controls are summarized in Table 3-5.

Table 3-5: Existing Security Controls

| | Existing Security Control |
|-----|--|
| 1. | Control sites support strong physical access control. |
| 2. | Remote sites support limited physical access control. |
| 3. | Backup capabilities support the majority of components and communications links. |
| 4. | The existing system employs a highly diverse range of components and communications links. This diversity inherently lowers the likelihood of a single attack causing system-wide failure. |
| 5. | The majority of communications links rely on dedicated connections. |
| 6. | Many of the communications protocols used are proprietary. |
| 7. | The majority of components are based on custom or little-used hardware and software which have traditionally avoided the attention of virus writers and the like. |
| 8. | Laws exist that prohibit interference with critical national infrastructure and unlicensed use of spectrum. These laws act as a deterrent to would-be attackers. |
| 9. | Policies and procedures are in place for the pursuit of “phantom controllers”. |
| 10. | Informal procedures are used by controllers and pilots to identify “phantom controllers” and ignore communications whose integrity has been compromised. |
| 11. | See and avoid procedures and TCAS limit the ability of a “phantom controller” who has successfully established control of an aircraft to cause catastrophic incidents. |
| 12. | Emergency communications on a separate frequency dedicated to emergency communications are supported. |
| 13. | Many components support a number of levels of access control for MMC. |

| | Existing Security Control |
|-----|---|
| 14. | Many components support identification and authentication of technicians for MMC. |
| 15. | Existing test and evaluation (although not traditionally security focused) is performed. |
| 16. | Robust development procedures (although not traditionally security focused) are used during implementation of components. |
| 17. | Many components produce audit logs including audit records of security-related events. |
| 18. | Users and technicians are subjected to background checks when they are hired. |
| 19. | Surveillance is performed. This acts in part as a detective security control since it enables controllers to identify aircraft that are deviating from their established route. |
| 20. | Users and technicians receive security training. |
| 21. | Monitoring of the NAS Communication System is performed. |

3.2.3 Assessing NAS Communication System Security Risk

Assessing security risk involves assignment of threat severity and threat likelihood rankings to each identified security threat.

In this study, the rankings defined in Table 3-1 were used for threat severity and Table 3-2 for threat likelihood. Threat severity was assigned primarily by determining which safety hazards the threat might cause, and assigning the threat severity ranking based on the hazard class of the most serious associated hazard. Threat likelihood was assigned primarily by determining the difficulty in realizing the threat and causing the relevant safety hazards in light of the existing security controls identified in Table 3-5.

Once each threat has been assigned rankings for threat severity and threat likelihood, the threat is then identified as an unacceptable risk, a moderate risk requiring further consideration, or an acceptable risk based on Table 3-3.

The detailed results of this process are described in Appendix F. In summary:

- Unacceptable risk – 0 threats were considered to represent an unacceptable risk.
- Moderate risk – 26 threats were considered to represent a moderate risk requiring further consideration:
 - All of these threats had “high – severe” severity and “extremely remote” likelihood rankings
- Acceptable risk – 13 threats were considered to represent an acceptable risk.
 - 11 of these threats had “high-severe” severity and “extremely improbable” likelihood rankings and
 - 2 of these threats had “none” severity and “frequent” likelihood rankings.

Note: Existing security controls as specified in Table 3-5 are largely specific to the legacy nature of the existing system – dedicated links, proprietary protocols, custom platforms and the like. Should these controls be removed in the future, this will have a significant impact on the threat assessment, and will likely lead to a need for substantial new security requirements.

3.2.4 Treating NAS Communication System Security Risk

Treating security risk involves identifying any new security requirements needed to mitigate threats, which represent unacceptable or moderate risk. New security

requirements may include technical requirements that lead to updates to components, as well as requirements for further security analysis.

Although no threats, which represent as unacceptable risk, were identified by this effort, a number of threats, which represent a moderate risk requiring further analysis, were identified. To an extent this reflects the reality that security, unlike safety, was not a primary driver during the design, development, and deployment phases of legacy NAS components.

To address these moderate-risk threats, it is recommended that more detailed, domain-level security assessments should be carried out. These assessments will enable determination of whether or not any additional technical requirements are needed in order to reduce the risk posed by the moderate-risk threats.

Two of the moderate risk threats – T.DEVELOP.TRAPDOOR and T.ENTRY.SOFTWARE – stand out as concerns. Although each is assigned a severity ranking of “only” “high-severe” when the associated safety hazards are considered, the threats could also cause catastrophic financial impact. The relevant attack scenario involves embedding a “time bomb” into a software update during development or distribution. Once the software update is installed and the time bomb activated, all components of that type would be disabled. Cleverly done it is conceivable that the affected components may need to be returned to their supplier in order to be fixed. The worst case scenario would be significant disruption of the NAS communications capability for several weeks.

It is therefore appropriate to consider a NAS-wide approach to addressing T.DEVELOP.TRAPDOOR and T.ENTRY.SOFTWARE. Any approach is likely to involve both:

- Procedural controls such as review of the software source code and configuration management to ensure that the software version deployed matches the software version reviewed.
- Technical controls such as software signing to ensure that the software is not changed during distribution. Indeed, Multimode Digital Radios (MDRs) already support a software signing capability for this reason.

It is recommended that the FAA consider requirements in this area in order to further mitigate these two threats.

3.3 Security Analysis Conclusions

The SSTF performed a security threat analysis in order to provide a security baseline for the existing NAS Communication System.

Procedural conclusions: The security analysis performed was coordinated with the safety hazard analysis described in Section 2. In particular:

- A common functional breakdown of the system was used as a starting point for both the safety and security analyses.
- The severity of security threats was assessed based on consideration of which safety hazards the threat might cause.

- Any new requirements were coordinated to ensure that a minimal set of requirements was introduced, and that new security requirements had no adverse effect on safety and vice versa. (This turned out to be redundant since neither safety nor security identified any definitive new requirements.)

The coordinated approach to safety and security was considered to be quite effective from a security perspective. It may be desirable to refine this approach in the future – perhaps by integrating coordination with safety into future versions of the SCAP process, or by considering information security during aircraft safety certification.

Technical conclusions: No threats, which represent an unacceptable risk, were identified during the security threat analysis. However a number of threats representing a moderate risk were identified. Furthermore, it must be emphasized that this effort represented only a high-level security threat analysis and no audit of existing security controls was performed. Since security is often in the details, it is quite possible that significant security concerns remain that were not considered.

To address the limitations of a high-level security analysis like this, and to ensure further consideration of the moderate-risk threats, it is recommended that detailed, domain-level security threat analyses be performed as a follow-on activity including audits of existing controls and their operation.

It is also recommended that the FAA considers new procedural and technical requirements to address the possibility of insertion of malicious code into the NAS via software updates.